Privacy-Preserving Reverse Auctions for Energy Trading in Smart Grids

Vincenzo Agate*, Pierluca Ferraro*, Marco Morana*, Elena Toscano*, and Giuseppe Lo Re*
*Department of Engineering, University of Palermo, Palermo, Italy.
Email: vincenzo.agate@unipa.it, pierluca.ferraro@unipa.it, marco.morana@unipa.it, elena.toscano@unipa.it, giuseppe.lore@unipa.it

***Abstract*—The transition toward decentralized smart grid architectures has introduced new challenges in coordinating competitive energy markets while preserving the confidentiality of market participants. This work proposes a privacy-preserving reverse auction framework for energy procurement in smart grids, enabling a grid operator to select multiple competing providers without ever accessing their bids in the clear. The architecture combines the additively homomorphic Paillier cryptosystem with a semi-trusted Blind Helper, which holds the decryption key but only operates on blinded and obliviously permuted values, so that neither entity alone can link sensitive values to provider identities. Provider reputations are kept encrypted end-to-end and updated homomorphically after each delivery, preventing behavioral profiling by the operator. Winners are selected through a greedy reputation-aware protocol that iterates until the energy demand is covered, and are remunerated at a uniform clearing price that guarantees truthfulness and individual rationality while revealing no individual bid or reputation value.**

***Index Terms*—Smart Grid, Reverse Auction, Privacy-Preserving Computation, Homomorphic Encryption, Energy Trading, Secure Multi-Party Computation, Demand Response**

I. Long Abstract

The ongoing transition toward smart grid infrastructures is fundamentally reshaping how electricity is produced, distributed, and traded. Rather than relying on a small number of large centralized plants, modern power grids increasingly integrate distributed energy resources (DERs), including rooftop photovoltaic systems, battery storage units, and prosumers that can both consume and generate electricity [1]. This shift introduces new market dynamics in which a potentially large number of energy providers compete to supply electricity to grid operators or aggregators, calling for efficient, fair, and transparent market mechanisms. In this context, reverse auctions, in which the buyer (the grid operator) solicits offers from multiple sellers (the energy providers) and selects the most competitive ones, have emerged as a natural fit for automated energy procurement [2]. The same paradigm applies naturally to emerging renewable energy communities, where procurement decisions involve small prosumers for whom confidentiality concerns are even more pressing.

Despite their appeal, reverse auction mechanisms raise significant privacy concerns in competitive markets. An energy provider's bid typically encodes sensitive information, including its cost structure, generation capacity, and operational constraints. Exposing this data, even to the auctioneer, could enable market manipulation, discourage participation, and undermine the fairness of the procurement process [3]. The threat is amplified in repeated markets: by observing bids and outcomes across multiple auction rounds, the operator can build detailed behavioral profiles of individual providers, infer their cost dynamics, and treat them strategically. In smart city contexts where grid operators interact with heterogeneous and partially untrusted stakeholders, the confidentiality of both bids and reputations therefore becomes a first-class requirement rather than an optional safeguard. Existing approaches to privacy-preserving auctions often rely on either heavyweight secure multi-party computation (SMPC) protocols, which incur prohibitive communication overhead, or on fully trusted auctioneers, which introduce a single point of failure from both a security and a trust perspective [4]. This work addresses these limitations with a two-entity architecture comprising an *Auction Server* (AS), operated by the grid operator, and a semi-trusted *Blind Helper* (BH). The BH is the sole holder of the decryption key, but it is only ever exposed to values that have been blinded and obliviously permuted by the AS; conversely, the AS orchestrates the entire auction without the ability to decrypt anything. Under the standard assumption that the two entities do not collude, neither of them can individually link any sensitive value to a provider identity. An overview of the proposed framework is presented in Fig. 1. The cryptographic foundation of the system is the Paillier cryptosystem [5], a partially homomorphic scheme whose additive property lets the product of two ciphertexts decrypt to the sum of the underlying plaintexts, and the exponentiation of a ciphertext by

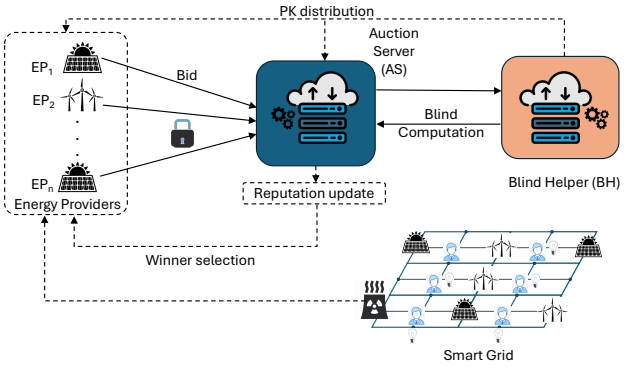

Fig. 1. Architecture of the proposed privacy-preserving reverse auction framework.

a public scalar to their scaling. These properties allow the AS to aggregate, scale, and re-randomize encrypted values with no decryption capability, while the operations that intrinsically require plaintext access (divisions, comparisons, maximum finding) are delegated to the BH in a controlled fashion, through multiplicative and additive blinding combined with oblivious permutations [6].

The system comprises three logical roles. **Energy Providers (EPs)** are the participants competing in the auction; each provider EP_i submits a sealed bid consisting of its offered unit price b_i and the energy volume c_i it can supply within the required delivery window, both encrypted under the BH public key. The **Auction Server (AS)** collects encrypted bids, orchestrates the winner determination protocol, performs all homomorphic manipulations, and publishes the auction outcome; it holds no decryption key. The **Blind Helper (BH)** generates and holds the Paillier key pair, distributes the public key, and performs the decryption-dependent steps of the protocol, always on blinded or permuted inputs; it is assumed to be semi-honest and not to collude with the AS. A distinctive feature of the proposed framework is that provider reputations are themselves confidential. Each provider is associated with an encrypted reputation $\mathcal{E}(r_i)$, with $r_i \in (0, 1]$, initialized to a default value at registration time and maintained by the AS exclusively in encrypted form: neither the operator nor the provider itself ever observes the plaintext reputation. Reputation enters the market mechanism through a reputation-adjusted score $v_i = b_i/r_i$, which effectively discounts the offers of historically reliable providers; the score is computed cooperatively, with the AS multiplicatively blinding the encrypted bid before involving the BH and homomorphically removing the blinding factor from the returned encrypted result, so that neither party observes b_i, r_i, or v_i in the clear.

The auction protocol unfolds in four phases. In **Setup**, the BH generates the Paillier key pair, retains the private key, and distributes the public key to the AS and to all providers, while encrypted reputations are initialized. In **Bid Submission**, each provider sends its encrypted pair $(\mathcal{E}(b_i), \mathcal{E}(c_i))$ to the AS, so that no plaintext bid ever leaves its system. In **Winner Selection**, the AS runs a greedy procurement loop over the encrypted reputation-adjusted scores $v_i = b_i/r_i$. At each iteration, the minimum-score candidate is identified through a secure argmin protocol based on double oblivious permutation, adapted from [6]: the AS permutes and scale-blinds the encrypted score vector, the BH applies a second internal permutation before decrypting, and returns the position of the minimum, thus learning only the *relative order* of anonymized values. The capacity of the winner is accumulated homomorphically, and an additive-blinding comparison returns to the AS a single boolean indicating whether the cumulated supply covers the demand D; the loop iterates until coverage. Finally, in **Clearing and Settlement**, all winners are paid a uniform clearing price equal to the critical score v_c of the marginal winner, cooperatively revealed by the BH. Since $r_i \leq 1$ implies $v_c \geq v_i \geq b_i$, individual rationality holds by construction, while the independence of the price from each winner's own bid yields truthfulness; crucially, the uniform price leaks no individual bid or reputation.

After delivery, each winner's reputation is updated according to the consistency between contracted and delivered energy, an externally observable quantity. The update term is computed in the clear by the AS using an asymmetric exponential weighting scheme that penalizes failures more than it rewards successes [7], then added homomorphically to $\mathcal{E}(r_i)$, with the final clamping delegated to the BH under additive blinding. The protocol is analyzed under the semi-honest model [8] with the standard AS–BH non-collusion assumption. Its leakage profile is explicit: the AS learns the winners, the number of iterations, and the clearing price; the BH learns only the relative order of doubly permuted, scale-blinded scores, unlinkable to identities; losing bids are never decrypted, and reputations are never exposed to any entity, providers included. Complementary economic (registration stake), structural (per-round limits), and statistical (anomaly detection) defenses further resist phantom-provider and Sybil attacks without affecting the cryptographic core.

In conclusion, the framework offers a deployable solution for privacy-preserving energy procurement in smart grids and renewable energy communities, combining Paillier encryption with lightweight blinding and oblivious-permutation protocols between two non-colluding entities to protect both bids and reputations, without a fully trusted auctioneer or heavyweight SMPC, while preserving truthfulness and individual rationality through a uniform-price rule. Future work will investigate zero-knowledge range proofs for bid well-formedness, distributed key generation to remove the single key holder, extensions to the malicious model, adaptation to continuous double auctions for real-time balancing markets, and mechanisms for assessing the trustworthiness of the Auction Server itself, for instance through auditable protocol transcripts or reciprocal reputation schemes for grid operators.

REFERENCES

[1] A. Timilsina, A. R. Khamesi, V. Agate, and S. Silvestri, "A Reinforcement Learning Approach for User Preference-aware Energy Sharing Systems," *IEEE Transactions on Green Communications and Networking*, 2021.

[2] Y. Mi, B. Tao, Y. Fu, X.-J. Su, and P. Wang, "A game bidding model of electricity and hydrogen sharing system considering uncertainty," *IEEE Transactions on Smart Grid*, vol. 15, no. 3, pp. 2751–2761, 2024.

[3] M. U. Hassan, M. H. Rehmani, and J. Chen, "Deal: Differentially private auction for blockchain-based microgrids energy trading," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 263–275, 2020.

[4] C. Ganesh, S. Gupta, B. Kanukurthi, and G. Shankar, "Secure vickrey auctions with rational parties," in *Proceedings of the ACM SIGSAC Conference on Comp. and Comm. Security*. ACM, 2024, p. 4062–4076.

[5] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International conference on the theory and applications of cryptographic techniques*. Springer, 1999.

[6] V. Agate, P. Ferraro, G. Lo Re, and S. K. Das, "Blind: A privacy preserving truth discovery system for mobile crowdsensing," *Journal of Network and Computer Applications*, vol. 223, 2024.

[7] V. Agate, A. De Paola, G. Lo Re, and A. Virga, "Reputation-based dissemination of trustworthy information in vanets," in *Mobile and Ubiquitous Systems: Computing, Networking and Services*. Cham: Springer Nature Switzerland, 2024, pp. 445–463.

[8] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game," in *Proceedings of the Nineteenth ACM Symp. on Theory of Computing, STOC*. ACM, 1987, pp. 218–229.